МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное
образовательное учреждение высшего образования
«Национальный исследовательский Нижегородский государственный университет
им. Н.И. Лобачевского»

Радиофизический факультет
(факультет / институт / филиал)

УТВЕРЖДЕНО
решением ученого совета ННГУ
протокол от
«31» мая 2023 г. № 6

Рабочая программа дисциплины

Основы информационной безопасности
(наименование дисциплины (модуля))

Уровень высшего образования
специалитет
(бакалавриат / магистратура / специалитет)

Направление подготовки / специальность
10.05.02 Информационная безопасность телекоммуникационных систем
(указывается код и наименование направления подготовки / специальности)

Направленность образовательной программы
Системы подвижной цифровой защищенной связи
(указывается профиль / магистерская программа / специализация)

Форма обучения
очная
(очная / очно-заочная / заочная)

Нижний Новгород

2023 год

1. Место дисциплины в структуре ООП

Дисциплина «Основы информационной безопасности» относится к дисциплинам обязательной части основной образовательной программы по специальности 10.05.02 «Информационная безопасность телекоммуникационных систем».

№ варианта	Место дисциплины в учебном плане образовательной программы	Стандартный текст для автоматического заполнения в конструкторе РПД
1	Блок 1. Дисциплины (модули) Обязательная часть	Дисциплина Б1.О.30 «Основы информационной безопасности» относится к обязательной части ООП специальности 10.05.02 «Информационная безопасность телекоммуникационных систем».

2. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями и индикаторами достижения компетенций)

Формируемые компетенции (код, содержание компетенции)	**Планируемые результаты обучения по дисциплине (модулю), в соответствии с индикатором достижения компетенции**		**Наименование оценочного средства**
	Индикатор достижения компетенции (код, содержание индикатора)	**Результаты обучения по дисциплине**	
ОПК-1. Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	ОПК-1.1. Знает: - понятия информации и информационной безопасности, характеристику ее составляющих - место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики - источники и классификацию угроз информационной безопасности - основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации	Знать: - сущность и понятие информации, информационной безопасности и характеристику ее составляющих - место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики, стратегию развития информационного общества в России - методы классификации и средства оценки угроз информационной безопасности для объекта информатизации	Собеседование
	ОПК-1.2. Умеет: - определять активы	Уметь: - определять угрозы информационной	Задачи (практические

	организации (предприятия), подлежащие защите, - - классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности	безопасности для объекта информатизации - классифицировать защищаемую информацию	задания)

3. Структура и содержание дисциплины

3.1 Трудоемкость дисциплины

	очная форма обучения	**очно-заочная форма обучения**	**заочная форма обучения**
Общая трудоемкость	**3 ЗЕТ**	**___ ЗЕТ**	**___ ЗЕТ**
Часов по учебному плану	**108**		
в том числе			
аудиторные занятия (контактная работа): **- занятия лекционного типа** **- занятия семинарского типа (практические занятия / лабораторные работы)**	**32** **32**		
самостоятельная работа	**43**		
КСР	**1**		
Промежуточная аттестация – экзамен/зачет	**зачет**		

3.2. Содержание дисциплины

Наименование и краткое содержание разделов и тем дисциплины, **форма промежуточной аттестации по дисциплине**	**Всего (часы)**	В том числе				
		Контактная работа (работа во взаимодействии с преподавателем), часы из них				**Самостоятельная работа обучающегося, часы**
		Занятия лекционного типа	**Занятия семинарского типа**	**Занятия лабораторного типа**	**Всего**	
1. Нормативная база в области	6	2			2	4

информационной безопасности						
2. Основные понятия безопасности телекоммуникационных систем и автоматизированных систем обработки информации	8	4			4	4
3. Характеристики наиболее распространенных угроз безопасности	10	4			4	6
4. Политика безопасности. Модели политики безопасности	59	10		32	42	17
5. Достоверная вычислительная база	14	8			8	6
6. Критерии оценки безопасности	10	4			4	6
Итого:	107	32		32	64	43

Практические занятия (лабораторные работы) организуются, в том числе в форме практической подготовки, которая предусматривает участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью.

Текущий контроль успеваемости реализуется в рамках занятий, лабораторного типа.

4. Учебно-методическое обеспечение самостоятельной работы обучающихся

Контрольные вопросы и задания для проведения текущего контроля и промежуточной аттестации по итогам освоения дисциплины приведены в п. 5.2.

5. Фонд оценочных средств для промежуточной аттестации по дисциплине (модулю),

включающий:

5.1. Описание шкал оценивания результатов обучения по дисциплине

Уровень сформированности компетенций (индикатора достижения компетенций)	**Шкала оценивания сформированности компетенций**						
	не зачтено		**зачтено**				
Знания	Отсутствие знаний теоретического материала. Невозможнос	Уровень знаний ниже минимальных требований. Имели место	Минимально допустимый уровень знаний. Допущено много	Уровень знаний в объеме, соответствующем программе	Уровень знаний в объеме, соответствующем программе подготовки.	Уровень знаний в объеме, соответствующем программе	Уровень знаний в объеме, превышающем программу

	ть оценить полноту знаний вследствие отказа обучающегося от ответа	грубые ошибки.	негрубых ошибки.	подготовки. Допущено несколько негрубых ошибок	Допущено несколько несущественных ошибок	подготовки, без ошибок.	подготовки.
Умения	Отсутствие минимальных умений . Невозможность оценить наличие умений вследствие отказа обучающегося от ответа	При решении стандартных задач не продемонстрированы основные умения. Имели место грубые ошибки.	Продемонстрированы основные умения. Решены типовые задачи с негрубыми ошибками. Выполнены все задания но не в полном объеме.	Продемонстрированы все основные умения. Решены все основные задачи с негрубыми ошибками. Выполнены все задания, в полном объеме, но некоторые с недочетами.	Продемонстрированы все основные умения. Решены все основные задачи . Выполнены все задания, в полном объеме, но некоторые с недочетами.	Продемонстрированы все основные умения,решены все основные задачи с отдельными несущественным недочетами, выполнены все задания в полном объеме.	Продемонстрированы все основные умения,. Решены все основные задачи. Выполнены все задания, в полном объеме без недочетов
Навыки	Отсутствие владения материалом. Невозможность оценить наличие навыков вследствие отказа обучающегося от ответа	При решении стандартных задач не продемонстрированы базовые навыки. Имели место грубые ошибки.	Имеется минимальный набор навыков для решения стандартных задач с некоторыми недочетами	Продемонстрированы базовые навыки при решении стандартных задач с некоторыми недочетами	Продемонстрированы базовые навыки при решении стандартных задач без ошибок и недочетов.	Продемонстрированы навыки при решении нестандартных задач без ошибок и недочетов.	Продемонстрирован творческий подход к решению нестандартных задач

Шкала оценки при промежуточной аттестации

Оценка	Уровень подготовки
зачтено	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «превосходно», продемонстрированы знания, умения, владения по соответствующим компетенциям на уровне, выше предусмотренного программой
	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «отлично», при этом хотя бы одна компетенция сформирована на уровне «отлично»
	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «очень хорошо», при этом хотя бы одна компетенция сформирована на уровне « очень хорошо»
	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «хорошо», при этом хотя бы одна компетенция сформирована на уровне «хорошо»
	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «удовлетворительно», при этом хотя бы одна компетенция сформирована на уровне «удовлетворительно»

не зачтено	Хотя бы одна компетенция сформирована на уровне «неудовлетворительно», ни одна из компетенций не сформирована на уровне «плохо»
	Хотя бы одна компетенция сформирована на уровне «плохо»

5.2. Типовые контрольные задания или иные материалы, необходимые для оценки результатов обучения.

5.2.1 Контрольные вопросы

Вопросы	*Код формируемой компетенции*
1. Основные понятия безопасности АСОИ	ОПК-1
2. Классификация угроз информационной безопасности	ОПК-1
3. Характеристики наиболее распространенных угроз безопасности	ОПК-1
4. Вредоносные программы	ОПК-1
5. Избирательная политика безопасности	ОПК-1
6. Полномочная политика безопасности. Модель Белла-Лападула	ОПК-1
7. Управление информационными потоками	ОПК-1
8. Достоверная вычислительная база	ОПК-1
9. Механизмы защиты. Ядро безопасности. Монитор ссылок	ОПК-1
10. Идентификация, аутентификация и авторизация субъектов и объектов системы	ОПК-1
11. Контроль входа пользователя в систему и управление паролями	ОПК-1
12. Регистрация и протоколирование. Аудит	ОПК-1
13. Противодействие «сборке мусора»	ОПК-1
14. Контроль целостности субъектов. Модель Биба	ОПК-1
15. Принципы реализации политики безопасности	ОПК-1
16. Система документов США. Классы защищенности компьютерных систем МО США. Европейские критерии безопасности	ОПК-1
17. Руководящие документы ГТК РФ: "Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности". Классификация автоматизированных систем и требования по защите информации	ОПК-1
18. Общие критерии оценки безопасности информационных технологий. Стандарт безопасности ГОСТ Р ИСО/МЭК 15408-2002 "Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий"	ОПК-1
19. Практическое внедрение электронной цифровой подписи. Закон Российской Федерации №63-ФЗ "Об электронной подписи"	ОПК-1
20. Принципы и мероприятия обеспечения информационной безопасности при обработке персональных данных. Закон Российской Федерации №152-ФЗ "О персональных данных". Требования к защите персональных данных при их обработке в информационных системах персональных данных, утв. постановлением Правительства РФ №1119 от 01.11.2012	ОПК-1

5.2.2. Типовые тестовые задания для оценки сформированности компетенции ОПК-1

1. Пояснить пример представленных ПРД: Пользователю на диске будут видны и доступны только явно описанные каталоги.
2. Пояснить пример представленных ПРД: Применение атрибутов наследования.
3. Пояснить по каким характеристикам СЗИ «Аккорд» отнесено к определенному классу защиты.

5.2.3. Типовые задания/задачи для оценки сформированности компетенции ОПК-1

Задача 1. Реализовать политику разграничения доступа «Конфиденциальное делопроизводство» для двух пользователей Userl и User2 с домашними каталогами D:\U1 и D:\U2.

Задача 2. Разработать набор испытаний реализации правил разграничения доступа из задания 1.

Задача 3. Исследовать содержимое журналов комплекса «Аккорд». Выделить в них сеансы работы всех пользователей системы. Детально описать один сеанс любого пользователя.

6. Учебно-методическое и информационное обеспечение дисциплины

а) основная литература:

1. Романец Ю. В., Тимофеев П. А., Шаньгин В. Ф. - Защита информации в компьютерных системах и сетях. - М.: Радио и связь, 2001. - 376 с.
2. Грибунин В. Г., Чудовский В. В. - Комплексная система защиты информации на предприятии: учеб. пособие для студентов вузов, обучающихся по специальностям "Орг. и технология защиты информации", "Комплекс. защита объектов информатизации"
3. Малюк А. А., Пазизин С. В., Погожин Н. С - Введение в защиту информации в автоматизированных системах: учеб. пособие. - М.: Горячая линия - Телеком, 2001. - 148 с.

б) дополнительная литература:

1. Садердинов А. А., Трайнев В. А., Федулов А. А. - Информационная безопасность предприятия: учеб. пособие. - М.: Изд.-торговая корпорация "Дашков и К", 2005. - 336 с.
2. Информационный менеджмент: учебник./Абдикеев Н. М., Бондаренко В. И., Киселев А. Д., Китова О. В., Лавлинский Н. Е., Попов И. И. - М.: ИНФРА-М, 2012. - 400 с.

в) программное обеспечение и Интернет-ресурсы:

1. Доктрина информационной безопасности Российской Федерации. Утверждена указом Президента Российской Федерации от 05.12.2016 г. № 646 (интернет-ресурс: http://www.kremlin.ru/acts/bank/41460)
2. Закон РФ от 21.07.1993 N 5485-1 «О государственной тайне» (интернет-ресурс: http://www.consultant.ru/document/cons_doc_LAW_2481/)
3. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ (интернет-ресурс: http://www.consultant.ru/document/cons_doc_LAW_61798/)
4. Федеральный закон «Об электронной подписи» от 06.04.2011 N 63-ФЗ (интернет-ресурс: http://www.consultant.ru/document/cons_doc_LAW_112701/)
5. Федеральный закон «О персональных данных» от 27.07.2006 N 152-ФЗ (интернет-ресурс: http://www.consultant.ru/document/cons_doc_LAW_61801/)

7. Материально-техническое обеспечение дисциплины

Помещения представляют собой учебные аудитории для проведения учебных занятий, предусмотренных программой, оснащенные оборудованием и техническими средствами

обучения.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечены доступом в электронную информационно-образовательную среду.

Программа составлена в соответствии с требованиями ФГОС ВО по специальности 10.05.02 «Информационная безопасность телекоммуникационных систем».

Автор (ы) _____ Л.Ю. Ротков

_____ А.А. Горбунов

Заведующий кафедрой «Безопасность информационных систем» _____ Л.Ю. Ротков

Программа одобрена на заседании методической комиссии радиофизического факультета от «25» мая 2023 года, протокол № 04/23.